PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/08, 19/10, H04L 9/00 — A1

(11) International Publication Number: WO 98/37513

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/AU98/00106

(22) International Filing Date: 20 February 1998 (20.02.98)

(30) Priority Data:
PO 5218 20 February 1997 (20.02.97) AU

(71) Applicant *(for all designated States except US)*: TELSTRA R & D MANAGEMENT PTY. LTD. [AU/AU]; 242 Exhibition Street, Melbourne, VIC (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: JOHNSON, Andrew [AU/AU]; 21 Sunbury Crescent, Surrey Hills, VIC 3127 (AU). BIGGAR, Michael [AU/AU]; 24 Kalbar Road, Research, VIC 3095 (AU).

(74) Agents: LESLIE, Keith et al.; Davies Collison Cave, 1 Little Collins Street, Melbourne, VIC 3000 (AU).

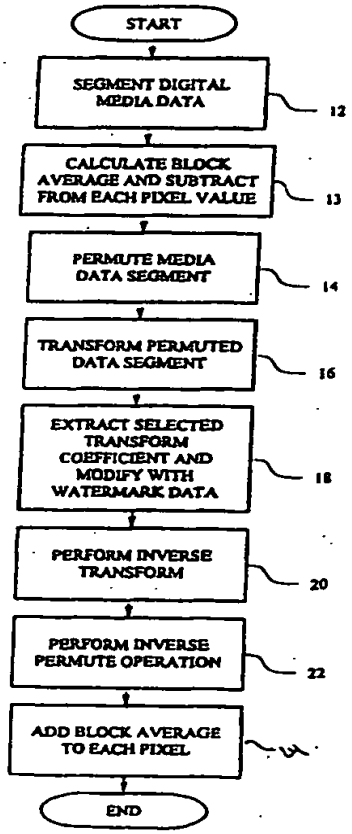
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: INVISIBLE DIGITAL WATERMARKS

(57) Abstract

A method and system of insertion and extraction of identification or authentication (watermark) data in digital media data such as video. The video data is divided into blocks and a pseudo-random function, such as a permutation, is applied thereto. The permuted data block is then transformed using an orthogonal transform such as a Walsh Hadamard Transform or a Discrete Cosine Transform. One or more of the ac coefficients generated by the transform are selected and the watermark data is inserted or extracted therefrom. An inverse permutation and inverse transform can then be used to return the video to the unencoded spatial domain. The inserted watermark data is substantially invisible in the reconstructed video since it is spread over the pixels in the block by virtue of the permute and transform.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INVISIBLE DIGITAL WATERMARKS

This invention relates to the provision of identification or authentication data, sometimes referred to as a watermark or signature, in digital media data such as digital image or audio data. In particular, the present invention relates to a method and apparatus for incorporating a watermark in digital media data, and a method and apparatus for retrieving or extracting a watermark from digital media data in which a watermark has been previously incorporated.

In this specification the term "watermark" is used to refer to any distinctive or distinguishing data which may be used for identification or authentication of the digital media data associated therewith, or of some attribute of the media data such as the source thereof. A watermark may comprise image data, such as pixel data forming a logo or the like, or may be in the form of coded text and/or binary numbers, for example, which represent a message. In some applications the watermark data may include error correction coding techniques to improve the robustness of the watermark to image manipulation. The format of the signal that is to be watermarked is not restricted to a multi dimensional representation. It is also possible for audio information to be watermarked. This method of encoding data is not restricted to information associated with copyright and could be used to convey any suitable information in a hidden manner.

Watermarks are utilised in media data for a number of reasons, one being to prevent or discourage copying of the media data if it is subject to copyright, or to at least allow for identification of the media data even if it is copied. Visible watermarks have been employed for many years in varying applications including banknotes and photographs, but have significant disadvantages because of their visible nature. Although a visible watermark may be quite effective in discouraging copying of an associated image, in general it is considered disadvantageous for a watermark to be obtrusive upon the original image.

Besides the issue of whether or not the watermark is visible in an associated image (or audible in the case of watermarked audio media), several other factors are also considered important.

For one, the watermark should be robust to manipulation of the watermarked media, and should be secure so as to not be easily removable by a malicious user. Before the advent of digital media processing and manipulation, a degree of robustness and security was inherent in a visible watermark, because a copy of the watermarked image would generally bring with it the visible watermark itself which would be difficult to remove. However, digital processing makes it possible to perform many sophisticated manipulative operations on watermarked media, which may degrade the visible watermark or be utilised to alter an image to at least substantially remove the watermark. In this case, therefore, the properties of a visible watermark count against the security thereof since it is clearly visible what must be removed or altered in the watermarked image. A paper entitled "Protecting publicly-available images with a visible image watermark" (Gordon Braudaway, Karen Magerlein & Fred Mintzer; SPIE Vol. 2659, pp 126-133) discusses robustness and security in visible image watermarks.

Visible watermarks are considered unsuitable for many modern applications because of the intrusive effect of the watermark on the original media. Watermarking schemes have been developed in which the watermark is substantially invisible on an original image but readily visible on a copy thereof. However, such schemes generally rely upon characteristics of photocopying or electronic scanning apparatus, and so are only suitable for a limited range of applications, such as in images or text on paper documents. In any event, these watermarking schemes are also subject to security difficulties arising from digital processing and manipulation.

In media involving a sequence of images, such as video media, it is particularly undesirable for a watermark to be intrusively visible, since considerable effort is expended in providing the image data to the user in a form which is as visually clear as possible, and a visible watermark may significantly detract from the original image. Visible watermarks are presently used in some video applications, particularly television coverage of live sporting events where a relatively small and faint logo or the like is superimposed on the television picture, typically near one corner thereof. This is not completely satisfactory, besides the

visual intrusion, because the logo can be easily cropped from the picture in a copy thereof, or could be relatively easily removed, at least substantially, with digital processing techniques. To make the visible watermark more secure it should be placed over the visually most important part of the image, which also makes the watermark more intrusive and thus less desirable.

Invisible watermarking techniques, particularly for digital media data, have been developed, and one is described in an article entitled "Watermarking Digital Images for Copyright Protection" (J.J.K. O'Ruanaidh, F.M. Boland & O. Sinnen). This article discloses a method of embedding a watermark in a digital image which is said to be invisible and quite robust. The image data is divided into rectangular blocks, and each block is then transformed using either a Walsh transform, discrete cosine transform (DCT) or wavelet transform. The bits defining the watermark graphic are inserted in the digital image by incrementing or decrementing a selected coefficient in the transform domain of the data block. Coefficients are selected according to a criterion based on energy content. Another algorithm described in the article relates to insertion of watermark data based on the use of the discrete Fourier transform (DFT). This method differs fundamentally from the transform domain technique outlined above. The DFT is a complex transform that generates complex transform domain coefficients given a real valued input. The watermark is placed in the phase component of generated transform coefficients when using this transform.

Another article which addresses the difficult issues of digital watermarking is "Secure Spread Spectrum Watermarking for Multimedia" (Ingemar J Cox, Joe Kilian, Tom Leighton & Talal Shamoon; NEC Research Institute, Technical Report 95-10). This article describes an invisible digital watermarking method for use in audio, image, video and multimedia data. The method described in this article also involves a frequency domain transform of the image data and insertion of the watermark data whilst in the transform domain. In practice, in order to place a length n watermark into an N x N image, the discrete cosine transform of the image is computed, and the watermark data encoded into the n highest magnitude coefficients of the transform matrix, excluding the dc component. In other words, the watermark data is placed

in transform domain components of greatest perceptual significance, which enables the watermark to be robust to image distortion and unauthorised removal without serious degradation of the image itself. This watermarking algorithm employs an energy compacting transform, which makes the selection of transform coefficients for encoding of the watermark data very important. For most images the coefficients selected will be the ones corresponding to the low spatial frequencies, with the result that significant tampering of the image at those frequencies would destroy the image fidelity before the encoded watermark. The watermarking techniques of J.J.K O'Ruanaidh et al and Ingemar J. Cox et al require the original image when performing the watermark extraction operation. As a consequence, proof of ownership is accomplished only if the original image is certified as being the original by a trusted third party, and the particular segment of the original image must be first identified and found before ownership is verified.

The present invention addresses some of the difficulties identified in the prior art, and embodiments of the invention aim to provide a digital watermarking process in which:

1. the presence of the watermark is invisible (i.e. the watermarked visual or audio material is visually or auditorially substantially indistinguishable from the original);

2. the watermark is robust to signal manipulation and distortion;

3. the watermark is secure;

4. the original media data is not required in order to extract the watermark; and

5. the watermark can be inserted and/or extracted by a simple computational procedure which can be done in real time.

In accordance with the present invention, there is provided a method for inserting identification or authentication data into digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform on the modified data block to obtain transform domain data;

modifying at least one selected transform domain data coefficient in accordance with identification or authentication data;

inverse transforming the transform domain data having the at least one modified coefficient; and

applying an inverse pseudo-random function to obtain watermarked digital media data.

The present invention also provides a method for extracting identification or authentication data from watermarked digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform to the modified data block to obtain transform domain data; and

extracting identification or authentication data from at least one coefficient of the transform domain data.

Preferably, the pseudo-random reversible function has the property of flattening the power spectral density of the data block (i.e. the function performs a spectral whitening operation), such that each coefficient then generated by the transform contributes substantially equally to the total energy of the block. This allows the watermarking process to be less sensitive, with regard to the introduced distortion, to the selection of the transform coefficient which is modified in the watermark insertion operation.

The insertion and/or extraction method can be performed in real time, which is particularly advantageous when the digital media data has presentation timing restrictions, such as in the

case of real time video and/or audio data.

It is preferred for optimal performance that the average (dc) component of the transformed media data be restricted to a single known transform coefficient and that this transform coefficient is not available for modification by the watermark insertion operation. It is also preferred that the pseudo-random reversible function be tolerant to the introduction of noise resulting from signal processing that could subsequently be performed on the watermarked media data. Many different pseudo-random functions could be used for this application. One pseudo-random function that offers good performance in terms of its noise rejection capability, spectral flattening performance and simplicity of implementation is a permutation of the data block based upon a keyed random number generator. In that case, the user should ensure that a permutation is selected that exhibits the desired spectral whitening characteristics as this is not guaranteed by all permutations.

A number of different transforms exist that could be used as the orthogonal transform operation in the preferred method. These include the Walsh Hadamard Transform (WHT), Discrete Cosine Transform (DCT), Discrete Sine Transform (DST) and Fast Fourier Transform (FFT). The Walsh Hadamard Transform is the preferred choice due in part to its low implementation complexity. The AC transform coefficients generated with such a transform in conjunction with an appropriate pseudo-random function, using real image data as input, are characterised by all possessing approximately equal energy. The selection of transform coefficient(s) for modification can thus be based on a random keyed operation to further enhance the security of the watermark.

For functions and transforms that do not restrict the average value of the data block to a single transform coefficient, it is preferred (to minimise watermark visibility) that the average (dc) value for the data block is calculated, stored, and subtracted from each data value in the data block prior to the application of the of the pseudo-random function. The average value is subsequently retrieved and added to each data value making up the watermarked data block immediately after the application of the inverse pseudo-random function.

The application of the pseudo-random function and the application of the orthogonal transform can be combined into a single operation. Similarly with respect to the inverse pseudo-random function and inverse transform. A combined data permutation and transform operation can be considered equivalent to, in the one dimensional case, performing a permutation upon the columns making up the basis matrix of the transform in question. Each permutation will yield an orthogonal transform, hence the number of transforms contained in the set is equal to the number of available permutations. Using this interpretation, the security of the watermark relies not just on which transform coefficient has been modified to contain the watermark data, but also on which member of the set of available transforms has been used.

The present invention further provides apparatus for inserting or extracting watermark data in digital media data, comprising:

segmenting means for segmenting the digital media data into data blocks;

processing means for applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block and performing a transform on the modified data block to obtain transform domain data; and

means for inserting or extracting watermark data in at least one coefficient of the transform domain data.

Preferably, in the case where watermark data is to be inserted in the digital media data the processing means is also adapted to perform an inverse transformation and inverse pseudo-random function on the transform domain data containing the watermark data so as to obtain watermarked digital media data.

In practice, the segmenting of the digital media data into data blocks might comprise forming blocks of 64x64 pixels of image luminance pixel data, where the watermark is to be inserted into a still image or image sequence. The block size need not be restricted to being square and of dimension 64x64 pixels, both smaller and larger block sizes are possible depending upon application requirements. In practice, the identification/authentication data which is

inserted into a data block of digital media data might comprise a pixel from a binary graphic, or data in the form of bits used to represent text and binary numbers, for example. The watermark data is inserted into the data block that has undergone a block transform operation. The distortion introduced due to the insertion of watermark data is dependent upon the block size, the number of transform coefficients modified by the insertion operation and the magnitude of the modification. The watermark data density per block is arbitrary depending upon application requirements. In general, however, the higher the density the more visually noticeable is the inserted watermark in the image. A series of data blocks may be contained in a single image frame or spread over a number of image frames.

The invention is described in greater detail hereinafter, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a flowchart illustrating operations for inserting watermark data into digital media data;

Figure 2 is a flowchart illustrating operations for extracting watermark data from digital media data;

Figure 3 is a diagram of the watermark insertion process of a preferred embodiment of the present invention;

Figure 4 is a flowchart illustrating the operations for a particular implementation of the watermarking insertion procedure;

Figure 5 is a block diagram of watermarking apparatus for real-time video; and

Figure 6 is a block diagram of a media monitoring system.

This invention relates to the insertion and extraction of identification or authentication data for use as a watermark in digital media data, such as digital image data, still or sequential, digital audio data or the like. A watermark provided in digital media data may provide a means for identification of the source or some other attribute of the media data as may be required to prove copyright ownership, for example. As mentioned above, embodiments of the present invention are designed to have a number of advantageous properties, including:

the watermark presence being at least substantially invisible (ie the watermarked visual

or audio material is visually or auditorially substantially indistinguishable from the original);

the watermark can be inserted and/or extracted by a simple computational procedure which can be done in real time for audio and/or video media data; and

the original media data not being required in order to extract the watermark from the watermarked media data.

Additionally, as also discussed above, it is desirable for watermarks in digital media data to also be both secure in that a malicious user cannot easily remove or disguise the watermark so as to prevent extraction, and robust to enable the inserted watermark to survive manipulation of the watermarked media data. Digital images and image sequences, for example, are seldom stored or transported over a communications link in their raw format. Frequently some form of compression may be applied to the media data, and it is therefore important that the signal processing associated with the compression algorithm does not remove or wash out the associated watermark inserted in the media data.

Although the following description of embodiments of the present invention refer primarily to still or sequential image data, it is to be understood that the invention is equally applicable to other forms of digital media data, such as digitised audio data.

In an embodiment of the invention, image pixel data is subdivided into 64 x 64 pixel spatial domain blocks in order to provide a manageable data segment in which to insert watermark data. For example, a digital image comprising 1,024 x 768 pixels may be nominally divided into blocks of 64 x 64 pixels so that the entire image is contained in an array of 16 x 12 image data blocks (a total of 192 data blocks). Different watermark data may then be inserted into each data block, so that the watermark data is spread over the entire image. For example, the watermark might comprise a 16 x 12 pixel logo or the like, so that a value representing each pixel of the logo is inserted in a respective data block of the digital image. Alternatively, the watermark may comprise a text message formed in ASCII code and/or binary numbers. A message comprising of 192 bits could be inserted in the digital image if a watermark density of 1/ 4096 (one bit per 64x64 block) was employed.

The invisibility and robustness of the watermark are aided by dividing the image into blocks and distributing the watermark data throughout the data blocks, and are further facilitated by the insertion procedure utilised to insert the watermark data into each data block. The following steps are used to insert a watermark data bit or binary pixel graphic into a 64 x 64 spatial domain luminance data block.

(i) Permute the 64x64 data block using a predetermined random permutation. There exist 4096 factorial different ways in which this permutation can be performed. To minimise the distortion introduced by the watermark modification, a permutation should be selected that performs a spectral whitening operation on a signal that has a predominant low pass power spectral density. The permutation is generated from a keyed pseudo-random operation.

(ii) Transform the permuted data using a Walsh Hadamard Transform. This transform can be implemented as a 4096-point one dimensional fast transform operation.

(iii) Watermark data is inserted into the data block by modification of selected transform coefficient(s). The coefficient selection process is based on a keyed-pseudo random operation, and does not include the dc coefficient in set of coefficients available for modification. To maximise security of the watermarking process, different coefficients are selected via the pseudo-random operation for each data block.

A watermark data bit can be represented by the sign of a selected transform coefficient. A transform coefficient value greater than or equal to zero could represent logic zero and the negative values logic one. Transform coefficient(s) need only be modified if necessary, to ensure that the sign (+/-) corresponds the digital bit to be embedded (1/0).

(iv) An inverse transform is then applied to reconstruct an approximation of the original

64x64 spatial domain data block. In the transform domain, the watermark data is completely contained by one transform coefficient when using a watermark data density 1/4096. In the spatial domain, however, the watermark data is distributed over each of the pixels making up the 64x64 data block.

The watermark read operation is accomplished by repeating steps (i) and (ii) above. The original image or image sequence is not required for the reading operation. The watermark data can be extracted with the knowledge of the permutation applied to the data block, the transform operation, and which of the transform coefficient(s) modified to contain the watermark data. The permutation employed is preferably kept secret by the owner of the image or image sequence. The permutation could be represented by a secret seed number to a well defined pseudo random number generator.

Block transforms such as the classic Walsh Hadamard Transform (WHT), Discrete Cosine Transform (DCT), Discrete Sine Transform (DST) and the Haar Transform (HT) can be employed in the watermarking process in embodiments of the invention. For transforms that isolate the average block value or dc value into one coefficient, that coefficient should not be used to contain watermark data. The WHT is the preferred choice for the transform operation due to its low implementation complexity. Fast transform implementations of the WHT exist that require only summing and one scaling operation, and the transform basis vector contains only +1 and -1 elements. The analysis and synthesis transforms are identical.

Figure 1 illustrates a flow chart of operation involved in insertion of watermark data into digital media data, according to an embodiment of the invention. Beginning at step 12, the digital media data is first segmented into manageable data blocks such as blocks of 64x64 pixels or equivalent data elements. Step 13 calculates the average pixel value for the block which is then subtracted from each pixel. Step 13 is unnecessary when using a transform that contains the block average in a single transform coefficient. This is the case with the WHT and the DCT, for example. The resulting dc transform coefficient should not, however, be used to contain watermark data. The media data block or segment is then subjected to a

permute operation (step 14) in which the data elements of the block or segment are rearranged in a pseudo random, but repeatable and reversible manner. Next, at step 16, the permuted spatial domain media data segment is subjected to the transform operation. In this embodiment one of the transform coefficients is selected and modified to include watermark data. When watermarking images or image sequences a watermark data bit could be represented by the sign of the selected transform coefficient. A transform coefficient value greater than or equal to zero could represent logic zero and the negative values logic one.

The watermark data density per block in this case is 1/4096. In some applications, densities greater than 1/4096 may be required.

Following insertion of the watermark data into the transform domain of the media data, the spatial domain media data is then reconstructed through steps 20, 22 and 23 by performing an inverse transformation followed by an inverse permute operation and then the previously subtracted block average value added to each pixel making up the block. Again, step 23 is not necessary when using a transform that contains the block average in a single transform coefficient. The resulting digital media data segment contains watermark data which is robust to manipulation thereof, secure from unauthorised removal, and yet the reconstructed, watermarked media data is substantially indistinguishable from the original spatial domain media data when compared in subjective quality testing.

In order to extract the watermark data form digital media data in which watermark data has been previously inserted, the procedure outlined in the flow chart of Figure 2 may be employed. Essentially this involves steps mirroring the first half of the procedure illustrated in Figure 1. The digital media data is first segmented as discussed previously (step 32), the average pixel value for that block is determined and subtracted from each pixel (step 33) if necessary. The resulting data block is then subjected to a permute operation as shown at step 34. The permute operation must be the same as that performed during insertion of the watermark data, and thus if different permute operations are variously employed, some record must be maintained of which of the particular 4096 factorial permutations applies to

the particular media data segment in question. This could be in the form of a secret seed to a well defined pseudo random number generator. The permuted media data segment is then transformed with the same transform used by the insertion operation (step 36). Then it is a simple matter to extract the particular coefficient for the transform domain media data and then recover from this the watermark information.

Figure 3 illustrates a block diagram of the watermark insertion process described in connection with the flow chart of Figure 1. As discussed above, in this embodiment only a single watermark data component, eg a data bit or binary graphic pixel, is inserted into each selected digital media data segment or block, and the information required to reconstruct an entire watermark requires the examination of a number of digital media data segments.

Figure 4 is a flow chart illustrating the insertion process of watermark data into digital media data, which has been segmented into data blocks, over a series of data blocks. Where the digital media data comprises a sequence of images, such as in the case of digital video or the like, a complete watermark (eg the total of the identification data) may in fact be distributed over more than one image or image frame. At step 42 the first data block in the image or sequence of images is selected and, if necessary, the average of that block is then calculated and subtracted from each pixel element in step 43. The resulting data block forming the image segment is subjected to a permute operation, as described hereinabove, at step 44. The permuted image data is then transformed using a block transform. At step 47 a particular transform coefficient is selected for possible modification. The selection process is performed in a pseudo random deterministic manner. Transforms that contain the block average (dc) in one transform coefficient, or set of coefficients, must eliminate this coefficient from the selection process. Step 48 performs the modification operation to incorporate the watermark data into the selected transform coefficient(s). The inverse of the transformation and permute operations are then applied at steps 50 and 52 and step 53 adds to each pixel value the average as determined in step 43, if necessary. A test is then applied at step 54 to determine whether the media data has finished, and if so the watermarking procedure ends. Otherwise, the next block of the digital media data is selected at step 56. The watermark data is then

incremented, meaning the next component of the watermark data, such as the next data bit or binary pixel element, is selected at step 58. Of course, it will be recognised that it is unnecessary for every data block of a particular digital media data source to be encoded with watermark data, and only a certain selection of data blocks may in fact be encoded with watermark data in practice. To provide copyright protection for the complete image sequence, the watermark can be repeatedly inserted, with the watermark beginning at different frame locations within the sequence and ensuring that watermarks do not overlap. Of course, acquisition of the signal is important. This can be accomplished, by incorporating in the watermark data, synchronisation information that, once acquired informs the watermark reader the location of the beginning of the watermark message data or binary graphic.

To increase robustness and ensure readability even in the case where the original video signal is significantly changed, such as through reduced spatial resolution or the case where watermarked interlaced material is later converted to non-interlaced format, the watermark can be distributed across both fields in such a way that the watermark can be independently read from either or both fields and/or restricted to the low spatial frequencies. The latter may be accomplished by the application of a 2x2 WHT on each row of the image to produce low and high spatial frequency components. The watermark is then inserted in only the half horizontal resolution frame corresponding to the low spatial frequencies. The full resolution watermarked frame is produced by performing an inverse 2x2 WHT on the rows making up the low spatial frequency watermarked half horizontal resolution frame and the original high spatial frequency half horizontal resolution frame.

In order to further improve security of the watermarking procedure, it is possible to alter the permute operation periodically (step 60 in Figure 4). As mentioned above, it is nevertheless necessary that the particular permute operation performed on each data block be repeatable at a future time to enable extraction of the watermark.

Figure 5 illustrates a block diagram of watermarking apparatus for encoding real time video with watermark data according to an embodiment of the present invention. Real time video

feed is provided to the apparatus at a buffer 80 or the like, which provides an input to real time processing circuitry 82. The circuitry 82 may comprise digital processing circuitry in the form of high speed programmable computer circuitry, for example, which carries out the algorithmic steps described in connection with Figure 4, for example. The watermark data is provided from a buffer 84 which may be in the form, for example, of a ring buffer which cyclically feeds watermark data being a component of watermark text or graphic material to the processing circuitry 82. The reconstructed video data containing the watermark data is then passed to an output buffer 86 which provides the video data for transmission, recording or whatever function the video data is required for.

Embodiments of the invention, operating in real time, can be utilised to add watermark data to media such as video and/or audio during live broadcast or other transmission, whilst recording to storage such as tape or disc, during broadcast or other transmission from storage, and during transferral from one storage device to another, for example. Furthermore, embodiments of the invention operating in real time can be used to monitor media such as television transmissions to detect the presence of watermark data incorporated in the media data. A block diagram of such a system is illustrated in Figure 6. Video data is provided to a buffer 90 from a source such as a broadcast receiver or the like. Real time processing circuitry 93 is coupled to receive the media data from the buffer 90 and perform the algorithmic steps described in connection with Figure 2, for example. This results in the extraction of any watermarking data contained in the media data which was inserted according to a process known to the monitoring apparatus (i.e. watermark data which has been added with a known permutation and transform in transform coefficients selected according to a known scheme). A comparison processor 94 can then be used to compare any watermark data which is retrieved with stored watermark data to determine if the retrieved watermark data corresponds to a known watermark indicating the source of the media data.

It will be appreciated from the foregoing description that the original media data is not required by the watermark extraction process in order to extract the watermark data, and therefore it is not required that the original image be certified by a trusted third party or held

in escrow in order to prove the presence of a watermark in the media data. Random accessibility of a watermark within an image sequence is easily achieved, as all that is required to extract the watermark is the image or sequence of images that contains sufficient watermark data to reconstruct the entire watermark or a substantial portion thereof, and the secret keys used to seed the random permutation and the random coefficient selection process.

The watermarking process according to an embodiment of the invention has been tested on still images and image sequences, and has been demonstrated to be near invisible to the naked eye in a comparison between the reconstructed, watermarked media data and the original media data. It has also be found to be secure and robust to compression such as 4 Mbps MPEG coding of image sequences and 20% quality setting for JPEG compressed still images. The described watermarking procedure is also robust to digital-to-analogue and analogue-to-digital conversions. Accordingly, embodiments of the invention can be utilised to insert and extract watermark data in analogue media as well as digital media. For example, watermark data can be inserted and extracted from broadcast or home quality analogue or digital video. Tests have been performed demonstrating a successful read operation for watermarked digital video originally of broadcast studio quality which has been temporarily recorded on an analogue consumer VHS tape. In the case where the media is generated, stored and/or transmitted in an analogue form, an analogue-to-digital conversion using known techniques is used to obtain digital media data before inserting or extracting the watermark data (see 92 in Figure 6). The media data may be returned to analogue form, if desired, using known digital-to-analogue techniques.

It will also be appreciated that the simple nature of the computational processes involved in the watermarking process of the present invention allow it to be applied quite readily to real time video data, for example. This is because the only two computationally complex steps in the watermarking procedure, namely the permute and transformation are still relatively simple. This makes for a watermarking process that is very low in complexity, is easily automated, and requires no human intervention in its application.

The foregoing detailed description of the present invention has been presented by way of example only, and is not intended to be considered limiting to the invention as defined in the claims appended hereto.

5

Claims:

1. A method for inserting identification or authentication data into digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform on the modified data block to obtain transform domain data;

modifying at least one selected transform domain data coefficient in accordance with identification or authentication data;

inverse transforming the transform domain data having the at least one modified coefficient; and

applying an inverse pseudo-random function to obtain watermarked digital media data.

2. A method as claimed in claim 1, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

3. A method as claimed in claim 1 or 2, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

4. A method as claimed in claim 1, wherein application of the pseudo-random function and application of the orthogonal transform are carried out in the same operation.

5. A method as claimed in claim 1, wherein the at least one transform domain data coefficient selected for modification is selected according to a keyed pseudo-random operation.

6. A method as claimed in claim 1, wherein a plurality of data blocks of the digital media data are modified according to the identification or authentication data.

7. A method as claimed in any one of claims 1 to 6, wherein the digital media data is video data.

8. A method as claimed in any one of claims 1 to 6, wherein the digital media data is audio data.

9. A method as claimed in claim 7 or 8, wherein the identification or authentication data is inserted into the digital media data in real time.

10. A method as claimed in claim 1, wherein at least one coefficient in the transform domain data which represents the average (dc) of the data block is restricted from selection for modification with the identification or authentication data.

11. A method as claimed in claim 1 or 10, wherein the orthogonal transform is a Walsh Hadamard transform.

12. A method as claimed in claim 1 or 10, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

13. A method as claimed in claim 1, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

14. A method as claimed in claim 1, including determining an average of data values in the data block, subtracting the average value from the data values in the data block before applying the pseudo-random function, and adding the average value back to the data values in the data block after applying the inverse pseudo-random function.

15. A method for extracting identification or authentication data from watermarked digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform to the modified data block to obtain transform domain data; and

extracting identification or authentication data from at least one coefficient of the transform domain data.

16. A method as claimed in claim 15, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

17. A method as claimed in claim 15 or 16, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

18. A method as claimed in claim 15, wherein application of the pseudo-random function and application of the orthogonal transform are carried out in the same operation.

19. A method as claimed in claim 15, wherein the extracting step includes selecting at least one transform domain data coefficient from which to extract identification or authentication data according to a keyed pseudo-random operation.

20. A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises video data.

21. A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises audio data.

22. A method as claimed in claim 20 or 21, wherein the identification or authentication data is extracted from the digital media data in real time.

23. A method as claimed in claim 15, wherein the orthogonal transform is a Walsh

Hadamard transform.

24. A method as claimed in claim 15, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

25. A method as claimed in claim 15, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

26. A method as claimed in claim 15, including determining an average of data values in the data block, and subtracting the average value from the data values in the data block before applying the pseudo-random function.

27. An apparatus for inserting or extracting watermark data in digital media data, comprising:

segmenting means for segmenting the digital media data into data blocks;

processing means for applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block and performing a transform on the modified data block to obtain transform domain data; and

means for inserting or extracting watermark data in at least one coefficient of the transform domain data.

28. An apparatus as claimed in claim 27, wherein the processing means is also adapted to apply an inverse transformation and inverse pseudo-random function of the transform domain data containing the watermark data so as to generate watermarked digital media data.

29. An apparatus as claimed in claim 27 or 28, wherein the apparatus inserts or extracts watermark data in digital media data in real time

30. An apparatus as claimed in claim 29, wherein the digital media data comprises video data.

31. An apparatus as claimed in claim 29, wherein the digital media data comprises audio data.

32. An apparatus as claimed in claim 27, including means for selecting at least one transform domain data coefficient for the insertion or extraction of identification or authentication data according to a keyed pseudo-random operation.

33. A media data monitoring system comprising:

a media data buffer for temporarily storing media data received from a data source;

a real time processor coupled to receive media data from the media data buffer and adapted to extract identification or authentication data according to the method defined in claim 15; and

a comparison processor coupled to the real time processor for comparing extracted identification or authentication data with known identification or authentication data.

34. A media monitoring system as claimed in claim 33, including an analogue-to-digital converter for converting media data into a digital form before processing by the real time processor.

35. A media monitoring system as claimed in claim 33 or 34, wherein the media data comprises video data.

36. A media monitoring system as claimed in claim 35, wherein the data source of the media data is a receiver of video transmissions.

37. A media data monitoring method comprising:

receiving media data from a data source;

extracting identification or authentication data according to the method defined in claim 15; and

comparing extracted identification or authentication data with known identification or

authentication data.

38. A media monitoring method as claimed in claim 37, including converting the media data into a digital form before processing by the real time processor.

39. A media monitoring method as claimed in claim 37 or 38, wherein the media data comprises video data.

40. A media monitoring method as claimed in claim 39, wherein the media data is received from a video transmission.

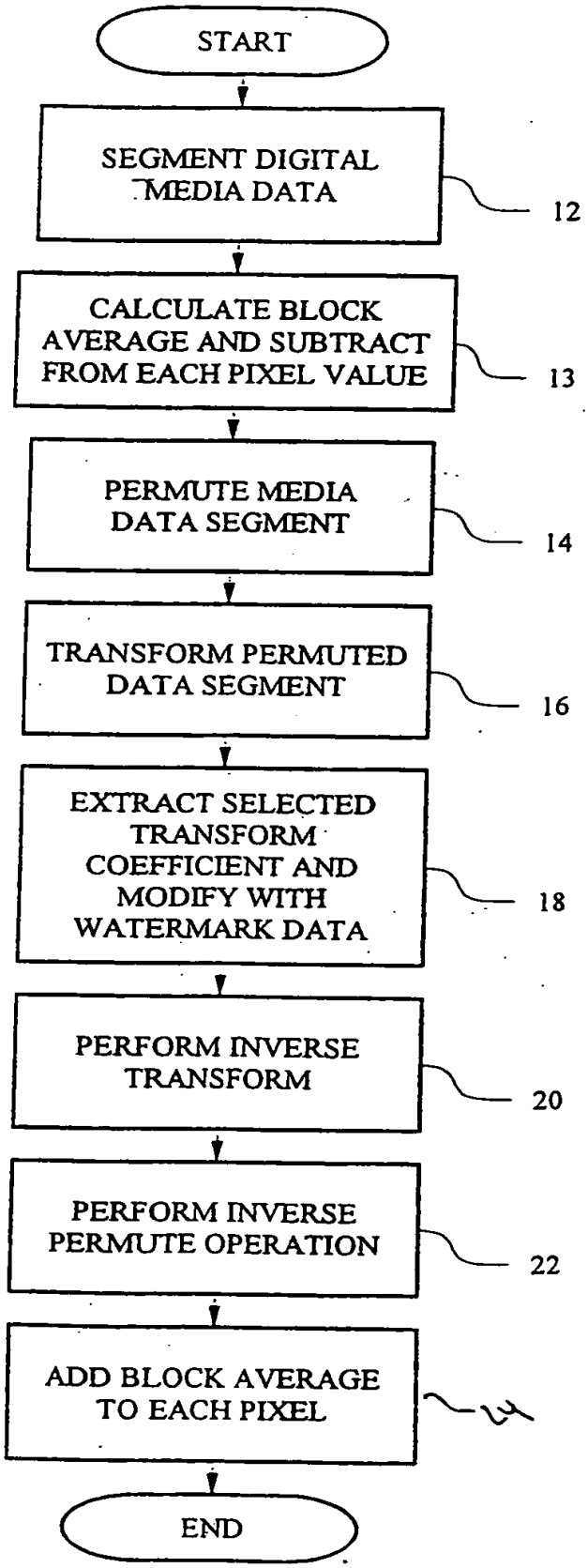


Figure 1.

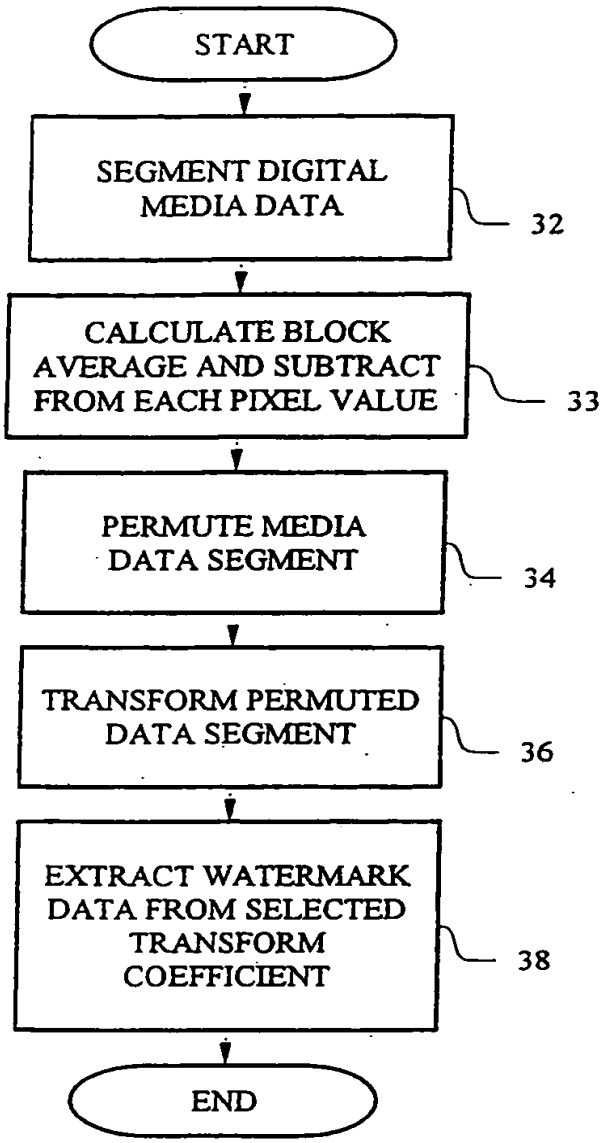


Figure 2.

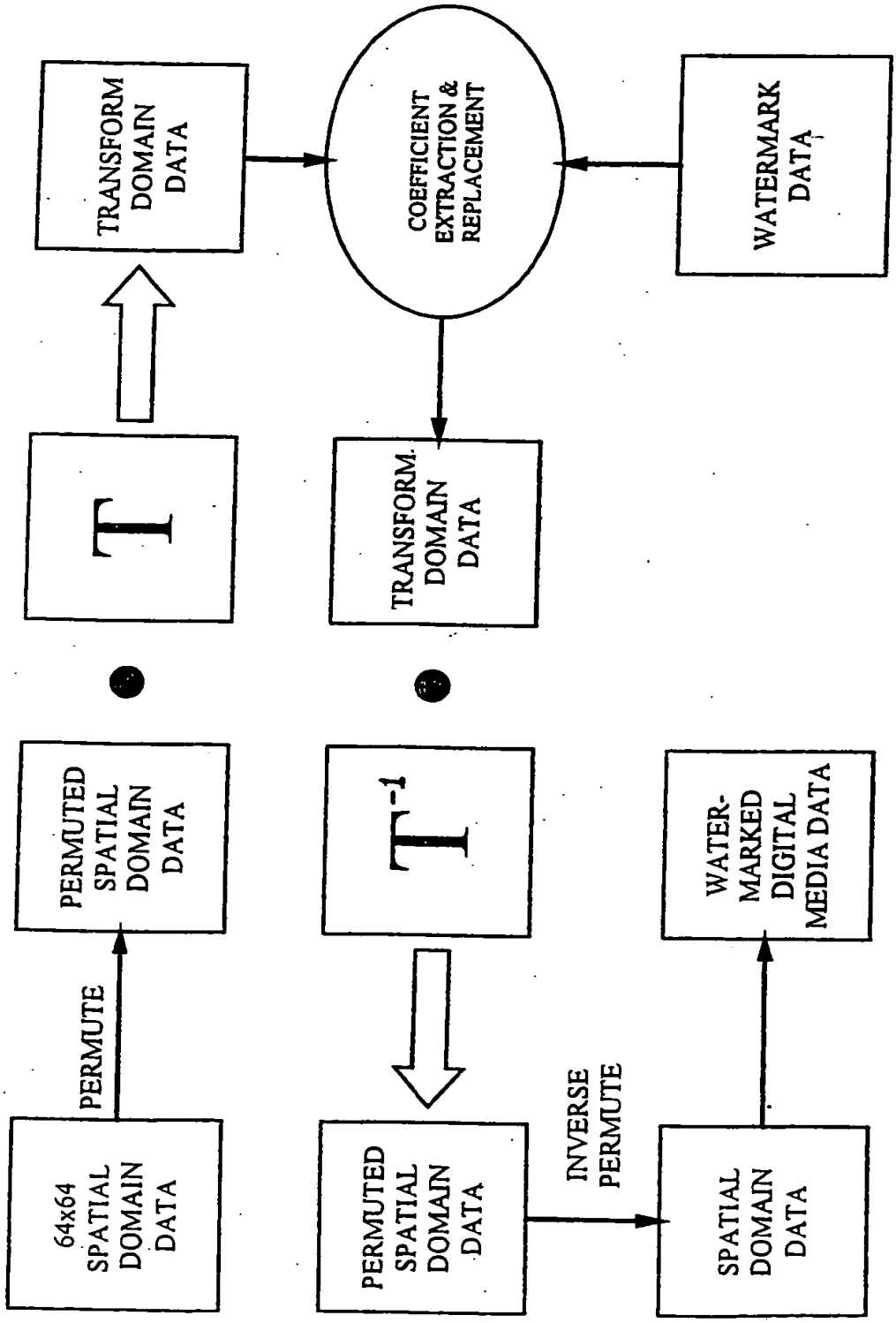

64x64 SPATIAL DOMAIN DATA
PERMUTE
PERMUTED SPATIAL DOMAIN DATA
T
TRANSFORM DOMAIN DATA
COEFFICIENT EXTRACTION & REPLACEMENT
WATERMARK DATA
TRANSFORM. DOMAIN DATA
T-1
PERMUTED SPATIAL DOMAIN DATA
INVERSE PERMUTE
SPATIAL DOMAIN DATA
WATER-MARKED DIGITAL MEDIA DATA

Figure 3.

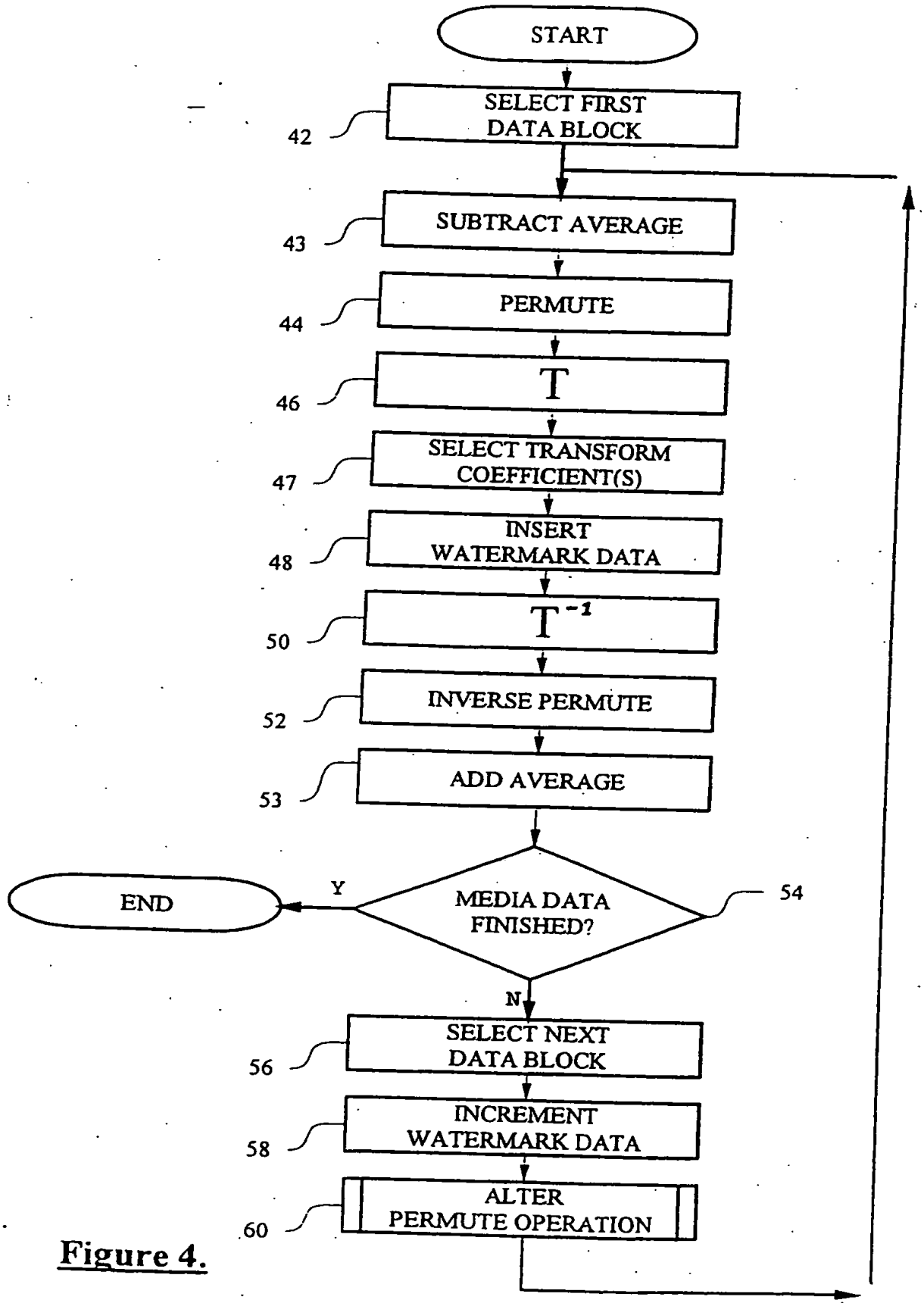

START
SELECT FIRST DATA BLOCK
42
SUBTRACT AVERAGE
43
PERMUTE
44
T
46
SELECT TRANSFORM COEFFICIENT(S)
47
INSERT WATERMARK DATA
48
T -1
50
INVERSE PERMUTE
52
ADD AVERAGE
53
MEDIA DATA FINISHED?
54
Y
END
N
SELECT NEXT DATA BLOCK
56
INCREMENT WATERMARK DATA
58
ALTER PERMUTE OPERATION
60

Figure 4.

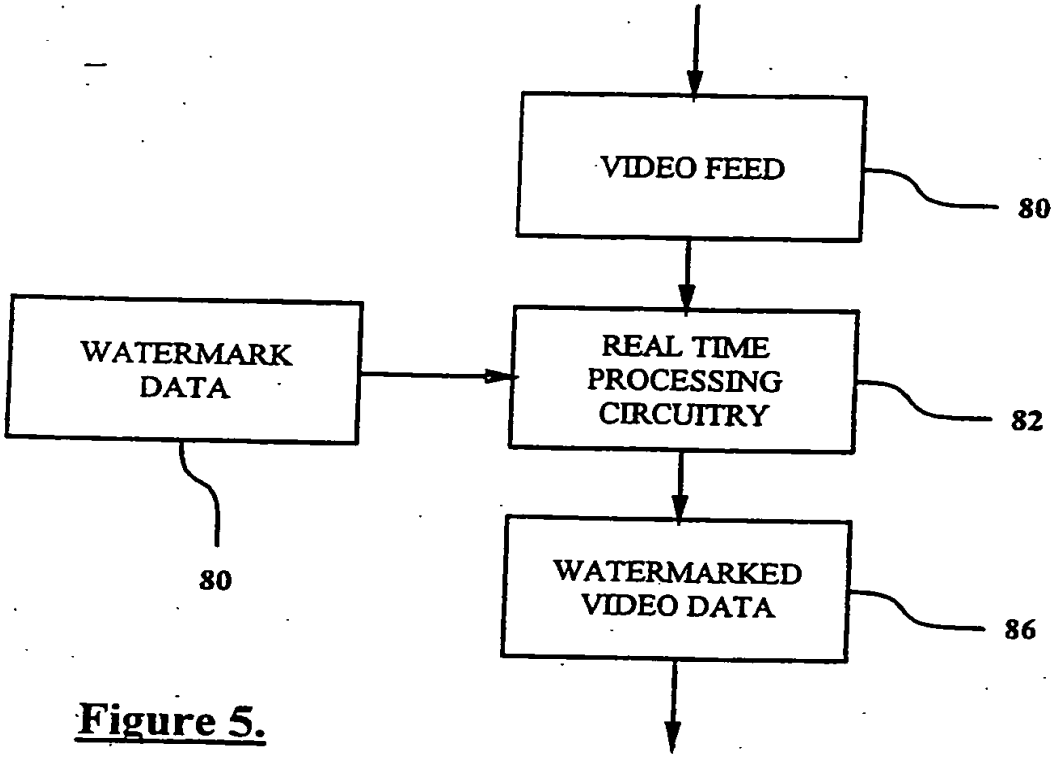


Figure 5.

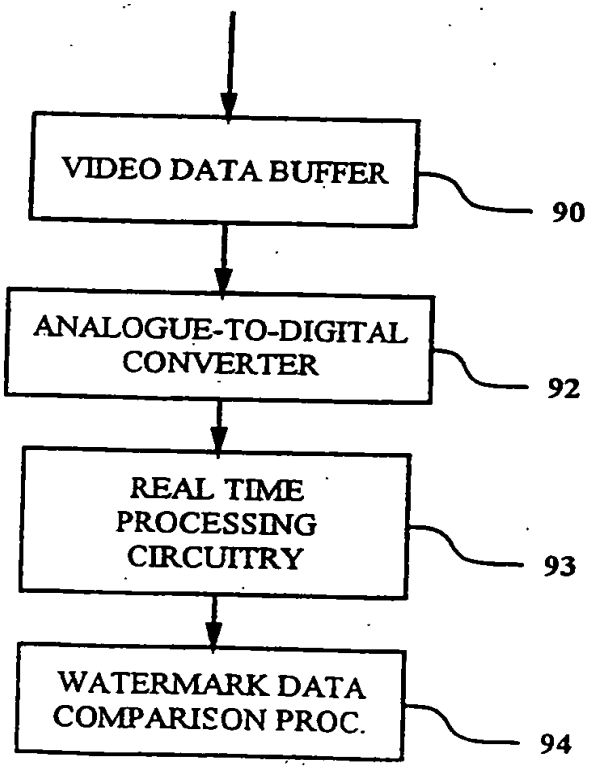


Figure 6.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 98/00106

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
EP	766468	AU	65840/96	CA	2184949	JP	9191394
AU	96/45073	WO	9617292	EP	795154		

END OF ANNEX

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00106

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: G06K 19/08, 19/10, H04L/9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC:as above

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU:IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IBM Patent Database: Digital, Watermark, Transform
Derwent WPAT:Digital, Watermark.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	EP 766468 (NEC CORPORATION) 2 April 1997	1 to 40
A	BYTE Magazine, January 1997, 'Look, It's Not There', Zhao, J. (INTERNATIONAL FEATURE) page 40is 7-12	1 to 40
X	AU 45073/96 (INTEL CORPORATION) 6 June 1996	33
X, T	AU 26083/97 (V-CAST INC.) 4 December 1997	33

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
17 March 1998

Date of mailing of the international search report
08 APR 1998

Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200
WODEN ACT 2606
AUSTRALIA
Facsimile No.: (02) 6285 3929

Authorized officer
J.W.THOMSON
Telephone No.: (02) 6283 2214